IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE: BPS DIRECT, LLC and CABELA'S, LLC, WIRETAPPING	**MDL NO. 3074** **2:23-md-03074-MAK**

DEFENDANTS' RESPONSE TO PLAINTIFFS' SUPPLEMENTAL MEMORANDUM

Pursuant to the Court's October 26, 2023 Order (ECF No. 71), Defendants BPS Direct, LLC and Cabela's, LLC submit the following response to Plaintiffs' Supplemental Memorandum (ECF No. 73).

Question 1 – Whether Website Users sufficiently alleged facts to establish Defendants accessed Website Users' computers without authority under 18 U.S.C. § 1030(a) with their best supporting authority:

In response to Question 1, Plaintiffs cite solely to one Central District of California case in arguing that they have adequately alleged unauthorized access of their computers under 18 U.S.C. § 1030(a). *See* ECF No. 73 at 3 (citing *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009)). The *Drew* case is not instructive to the analysis the Court must conduct here.

In *Drew*, the Court considered the question of "whether a computer user's intentional violation of one or more provisions in an Internet website's terms of services (where those terms condition access to and/or use of the website's services upon agreement to and compliance with the terms) satisfies the first element of section 1030(a)(2)(C)." *Id.* at 457. In other words, the case analyzed the conduct of an individual's unauthorized access of a company's website.

The conduct that Plaintiffs complain of is the exact opposite. Plaintiffs here seek to bring their claims based on actions that Defendants allegedly took, *on their own websites*. Neither Plaintiffs' briefing, nor the *Drew* opinion, explain how Defendants' alleged actions on their own websites constitute unauthorized access to *Plaintiffs'* computers. For the reasons discussed in Defendants' briefing, the Computer Fraud and Abuse Act claim should be dismissed.

Question 2: As to the wiretap claims under the federal, California, and Missouri laws, Website Users provide support for their argument that party status and consent exceptions do not apply and clarify whether Defendants are parties to the communications at issue.

Plaintiffs first argue that Defendants were *not* parties to all of the communications that were allegedly intercepted. ECF No. 73 at 5 (citing Compl. ¶¶ 1, 7, 90, 259, 268, 299, 312, 342, and 405 as "alleging instances of content captured without interaction.") But none of these paragraphs describes any communication between Plaintiffs and a party other than Defendants. To the contrary, they discuss "Plaintiff's and Class Members' electronic communications *with Defendants' websites*." Compl. ¶ 268 (emphasis added). Plaintiffs' cited authority demonstrates that, to the extent that Plaintiffs' website interactions constitute communications that can be intercepted, Defendants, as the website owners, are parties to those communications. *See Jurgens v. Build.com, Inc.*, 2017 WL 5277679, at *5 (E.D. Mo. Nov. 13, 2017) (finding that "[a]s a party to the communication, [the website owner] is exempt from liability under the [federal] Wiretap Act"). Neither Plaintiffs' memorandum nor their Complaint explains who the second party to their alleged communications at issue in this case would be, if not Defendants. Defendants were parties to the relevant communications here.

Plaintiffs also assert, without argument, that the scope of consent cannot be determined this early and that Plaintiffs never consented to the interceptions at issue. As discussed in Defendants' Motion to Dismiss, Plaintiffs consented and that consent can be determined at this stage of the litigation. ECF No. 54-1 at 21-25.

Question 3: As to the wiretap claims under the federal and Missouri laws, Website Users respond to Defendants' arguments and cited case law in support of their position Website Users fail to allege a criminal or tortious purpose (ECF No. 54-1 at 19-22, ECF No. 57 at 15-16):

Plaintiffs still do not squarely address the thrust of Defendants' argument regarding the criminal or tortious purpose exception to the exemption of wiretap liability for parties to a communication that, as alleged by Plaintiffs, Defendants' purpose for allegedly intercepting information through session replay code was "to maximize profits through predictive marketing and other targeted advertising practices." ECF No. 54-1 at 10 (citing Compl. ¶¶ 294, 337, 400, 439). Nor do they address the cases that Defendants cited in Defendants' briefing. (ECF No. 54-1 at 19-22, ECF No. 57 at 15-16).

For the reasons discussed in Defendants' briefing, Plaintiffs have failed to allege a criminal or tortious purpose under the federal and Missouri laws and those claims should be dismissed.

Question 4: As to the wiretap claims under the federal and Missouri laws, provide your best authority as to how we should consider applying the "criminal or tortious purpose" exception:

Plaintiffs' supplemental memorandum attempts to distinguish the *DoubleClick* case by pointing to the fact that the *DoubleClick* court noted that the cookies at issue there "only collect information concerning users' activities on DoubleClick-affiliated Web sites." ECF No. 73 at 9 (citing *In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 407, 504 (S.D.N.Y. 2001)). But that is, at most, precisely what Plaintiffs have alleged Defendants to have done here. Plaintiffs' entire complaint focuses on the information that the session replay code installed on Defendants' websites allegedly captured *while Plaintiffs visited Defendants' websites*.

Contrary to Plaintiffs' arguments elsewhere in their supplemental briefing, Plaintiffs' Complaint does *not* allege that Defendants' use of session replay code tracked any information from Plaintiffs' activities on other websites not owned by Defendants. The closest that any of the paragraphs that Plaintiffs cite to comes to doing so is a conclusory allegation that *some* session replay providers—not Defendants—can associate "fingerprints" with some users identities across websites. Compl. ¶¶ 78-80. But even these conclusory allegations do not suggest that Defendants here have engaged in anything close to the wide-spread tracking across all web pages visited by individuals, despite their decisions to use a private browsing mode, that was alleged in *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1055-56 (N.D. Cal. 2021).

Question 5 – As to the wiretap claims under the Maryland and Massachusetts laws, describe whether and to what extent our analysis differs given the definitions of "contents" under each State's law:

Plaintiffs' cited authority does not require the Court to find that the information Plaintiffs allege was captured here constitutes "contents" under either the Maryland or Massachusetts laws. First, in *Commonwealth v Du*, the Massachusetts Appellate Court found that a video recording of a criminal defendant was "contents" and should have been suppressed under the wiretap statute because the video "shows the defendant while he was having [] oral communications with the undercover officer and, accordingly, is 'information concerning the identity of the parties to such communication.'" 103 Mass. App. Ct. 469, 481 (2023). None of the information that was allegedly captured by the session replay code here is analogous to a video recording of Plaintiffs.

Second, in *Alves v. BJ's Wholesale Club, Inc.*, 2023 WL 4456956 (Mass. Super. June 21, 2023), the trial court's opinion there did not address the argument Defendants make here that mere allegations of how session replay code works *generally*, are insufficient to state a claim where Plaintiffs do not plausibly allege that Defendants configured the session replay code on their websites to actually capture information regarding Plaintiffs' identity. The actual allegations that Plaintiffs rely on in their memorandum are limited to general allegations about the potential capabilities of session replay code generally. *See* ECF No. 73 at 11 (citing Compl. ¶¶ 76-78).

Plaintiffs do not adequately allege that the relevant information here constitutes "contents" under either the Maryland or Massachusetts statutes.

Question 6 – As to the wiretap claims under the federal, California, and Maryland laws, provide your strongest authority as to whether Website Users allege a contemporaneous interception:

The cases that Plaintiffs cite in response to Question 6 are inapposite as none of those cases consider allegations, like those present here, that the communications at issue were "accumulated" by the defendant before being sent to a third party (Compl. ¶ 68), rather than being intercepted in transit. *See Luis v. Zang*, 833 F.3d 619, 630 (6th Cir. 2016) (allegations that communications were "immediately and instantaneously" copied and sent); *Garcia v. Yeti Coolers, LLC*, 2023 WL 5736006, at *4 (C.D. Cal. Sept. 5, 2023) (allegations of "real time" collection of internet chat messages); *Valenzuela v. Nationwide Mut. Ins. Co.*, 2023 WL 5266033, at *5 (C.D. Cal. Aug. 14, 2023) (same); *Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073, at *4 (N.D. Cal. June 9, 2023) (allegations of real time interception that were not "squarely contradict[ed by] Plaintiffs' otherwise plausible allegation[s]").

Further, this issue can be decided at the motion to dismiss stage because the fact that these transmissions are not contemporaneous is based on *Plaintiffs' own allegations*. Plaintiffs are correct that the Court must accept Plaintiffs' allegations as true at this stage, but Plaintiffs allege that the alleged communications were "accumulated" and then forwarded "in blocks periodically throughout the user's website session." Compl. ¶ 68.

Question 7 – As to the wiretap claims under the Maryland, Massachusetts, and Pennsylvania laws, provide your strongest authority as to whether session replay software is a "device":

Plaintiffs do not provide any cases that are binding on this Court where session replay code has been found to be a "device" under the Maryland, Massachusetts, and Pennsylvania laws. As discussed more fully in Defendants' briefing, in the absence of such binding authority to the contrary, under normal principles of statutory interpretation, snippets of JavaScript code are not a "device" under these statutes. ECF No. 54-1 at 15-18; ECF No. 57 at 11-12; ECF No. 72 at 6.

Question 8 – As to the invasion of privacy claims, Website Users shall address the impact, if any, of *Kurowski v. Rush System for Health*, No. 22-5380, 2023 WL 2349606 (N.D. Ill. Mar. 3, 2023) and respond to Defendants' arguments (ECF No. 54-1 at 37, ECF No. 57 at 21):

Contrary to Plaintiffs' assertions, the court in *Kurowski v. Rush System for Health*, did not hold that an intrusion upon seclusion claim fails whenever there is an alleged disclosure. 2023 WL 2349606 (N.D. Ill. Mar. 3, 2023). Rather, the *Kurowski* court dismissed the intrusion upon seclusion claims there because, to the extent there was an intrusion on the *Kurowski* plaintiff's intrusion, any such "intrusion upon patients' seclusion, via interception of their communications, is carried out by third parties." *Id.* at *9. The same is true here. Plaintiffs allege that their voluntary communications with Defendants were intercepted by a third-party. They do not allege an intrusion *by Defendants*.

The *Feldman v. Star Tribune Media Company LLC* case Plaintiffs cite did not involve an intrusion upon seclusion claim (or any other invasion of privacy claim). 2023 WL 2388381, at *4 (D. Minn. Mar. 7, 2023). The portion of the case Plaintiffs cite discusses whether a violation of the Video Privacy Protection Act "bears a close relationship" to the common law claim of intrusion upon seclusion for purposes of Article III standing. *Id.* It does not discuss whether allegations of any kind, much less allegations similar to those at issue here, adequately state a claim for intrusion upon seclusion under the laws of any state.

Question 9 – As to the claim under the California Unfair Competition Law, Website Users shall address the impact, if any, of *Moore v. Centrelake Medical Group*, 83 Cal. App. 5th 515 (Cal. App. Ct. 2022) on their standing arguments and respond to Defendants' arguments (ECF No. 54-1 at 44-45, ECF No. 57 at 23):

The California Appellate Court in *Moore v. Centrelake Medical Group*, 83 Cal. App. 5th 515 (Cal. App. Ct. 2022) made clear that in order for a diminution of value theory to support UCL standing, a plaintiff must allege "that a market for [the data] existed" and that they "attempted or intended to participate in this market, or otherwise to derive economic value from their PII." *Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515, 538, *review denied* (Dec. 14, 2022). Plaintiffs reliance on *Calhoun v. Google*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021) and District of Nevada case law rejecting this requirement do not require the Court to ignore this guidance from the California Appellate Court.

As noted in Defendants' prior briefing, the *Calhoun* opinion is an outlier and "[t]he weight of the authority in the [Northern District of California] and the state, however, point in the opposite direction: that the mere misappropriation of personal information does not establish compensable damages" for UCL standing. *Katz-Lacabe v. Oracle Am., Inc.*, 2023 WL 2838118, at *8 (N.D. Cal. Apr. 6, 2023) (collecting cases).

Question 10 – As to Plaintiff Tucker's claim under the Missouri Merchandising Practices Act, Website Users shall provide support for their argument the Act is not limited to consumers who make purchases in the marketplace:

Plaintiffs' citation to *Ports Petroleum Co. Inc. of Ohio v. Nixon*, 37 S.W.3d 237, 240 (Mo. 2001) has no bearing on the question of whether an individual needs to make a "purchase" to be able to bring a claim under the Missouri Merchandising Practices Act ("MMPA"). The *Ports* opinion does not involve an individual bringing a private suit under the MMPA and the Missouri Supreme Court was not presented with the issue that is relevant here. *Id.*

For the reasons discussed in Defendants' briefing, the MMPA claim should be dismissed.

CONCLUSION

For these reasons, and those contained in Defendants' Motion and Reply Brief, Plaintiffs' Complaint should be dismissed in its entirety.

November 7, 2023

Respectfully Submitted,

By: */s/ Jennifer A. McLoone*

Erin (Loucks) Leffler (PA ID No. 204507)
Shook, Hardy & Bacon L.L.P.
Two Commerce Square
2001 Market St., Suite 3000
Philadelphia, PA 19103
Phone: (215) 278-2555
Fax: (215) 278-2594
eleffler@shb.com

Jennifer A. McLoone (admitted *pro hac vice*)
Shook, Hardy & Bacon L.L.P.
201 South Biscayne Boulevard
Suite 3200
Miami, FL 33131-4332
Phone: (305) 358-5171
Fax: (305) 358-7470
jmcloone@shb.com

Maveric Ray Searle (admitted *pro hac vice*)
Shook, Hardy & Bacon L.L.P.
111 South Wacker Drive
Suite 4700
Chicago, IL 60606
Phone: (312) 704-7741
Fax: (312) 558-1195
msearle@shb.com

Counsel for Defendants